Beate Rössler

The Value of Privacy

Privacy and its violations are at the moment an extraordinarily controversial theme for a variety of reasons: since September 11, 2001 on the one hand because Western governments are now trying to prevent terrorist attacks by collecting detailed data on citizens and subjecting it to intense scrutiny using sophisticated techniques. And on the other hand—and on a very different plane—because TV shows such as *Big Brother* seem to take the concept of the protection of the private realm to its logical extremes.

We are dealing here with a paradoxical situation where socially critical voices are complaining that people have no interest any more in their private sphere, while the very same people proclaim in the same breath that people have such a strong interest in their privacy that the new anti-terrorism laws, for example, or the new information technologies in general represent a constant violation or at least an imminent threat to their right to the privacy of their personal information.

[...]

I would like to start off with a few remarks on the concept we call "private" and what it means. In fact, we speak of privacy or private in entirely divergent contexts: religion is a private matter just as certain data, for example medical data, is my own private concern; the clothes I wear and the occupation I choose are private matters; and my own apartment is also of course private: *prima facie,* all of these things have no more to do with each other than this label. If we look closer, however, we can see that all these forms of privacy have to do with a person exercising control over access—to her home, but also to her personal data or to her decisions, such as the right to decide which religion to belong to (if she wants to belong to one at all).

The common denominator for all these forms of privacy would thus be access control: something is private when I *am in a position to and have a right to* control access to it—whether to data, to a home, to decisions or to ways of acting. This "access" can of course be meant metaphorically, such as in the case of access in the sense of *the right to object to* decisions; access can also be meant quite literally as access to data or admission to my home. Privacy as access control can thus have varying meanings.

Something else then becomes clear here: that it would seem to make sense to divide the complexity of privacy into three dimensions: if we are speaking of data about a person, i.e. in general of what others know about me, then we mean *informational privacy.* If it is a matter of my private decisions and actions, then we are talking about my *decisional privacy;* and if the privacy of my own four walls is at stake, I then refer to my *local privacy.* I regard these three dimensions of privacy as exhaustive, because I believe that by means of this tripartite definition all problems and phenomena of privacy can be described and analyzed.

[...]

Despite the heterogeneity of the ways the term "private" is applied, and irrespective of the differences between the three dimensions of the private, we can still distinguish a common denominator by asking what this privacy is supposed to protect in each case. The answer is that privacy protects individual freedom and personal autonomy. We want our privacy to be protected because we can otherwise not lead our lives with the greatest possible degree of freedom and self-determination. And it is for precisely this reason that we *should* value our privacy, because by (involuntarily) giving up our entitlement to privacy we also give up certain rights to be free and self-determined.

[...] What, then, is the value of privacy? Why are we unable to, and have no desire to, conceive of a society without privacy, such as in Orwell's *1984*?

I will use the modern concept of autonomy and self-determination here, autonomy in its broadest sense, which has to do with the fundamental idea that every person can and should be allowed to decide for herself how to live. To be "free" and autonomous in this sense means to choose how we live and how we want to be. Autonomy here also means being able to give yourself good reasons for why you live your life the way you do, and to take as much responsibility as possible for your own decisions and way of life.

[...]

Now, this kind of autonomous life requires certain conditions—conditions that have to do with people's subjective abilities as well as with interpersonal and social circumstances. Among these conditions are—and here I can of course only briefly list some keywords—a democratic society constituted upon respect for the autonomy of subjects and the protection of this autonomy; this includes the possibility of living according to autonomous decisions and life plans; it includes the existence of social opportunities and options that can be taken advantage of by all; it includes the protection of intimate relationships in which autonomy can be learned and lived; such protection is also necessary because people can only make existential and autonomous decisions in this kind of protected environment. Even if we only roughly outline the social conditions that allow for the possibility of an autonomous life as above, we already immediately notice that the protection of privacy is a constituent part of such a life: decisional privacy because otherwise decisions and life plans cannot be lived out and pursued. Local privacy because otherwise the protection of intimate relationships and the possibility to retreat into a private realm are not ensured.

I will now elucidate the connection between autonomy and privacy in more detail based on the problem of *informational privacy.* What we first of all need to do in order to understand this concept is to define it as broadly as possible. In my opinion, informational privacy namely goes beyond data protection by the state, the police and commerce, but is also important in all social relations in which subjects live. This broad concept becomes evident when one considers the following questions:

Why do we in general deem it inappropriate, impolite, immoral or even illegal when others observe or eavesdrop on us against our will and without our being aware of it (or even if we do know about it), or even go so far as to film us or tape what we say, whether at home, at the office, on the street or in a café? Why do we then feel disturbed, ashamed, violated, impaired, insecure, controlled, when we notice it? What is wrong with companies handing out personal data; or why do we object to close friends telling others something about us they only know because we are so close? These are the kinds of questions that demarcate the outlines of the issue and the problem of possible violations of informational privacy, because all of these questions refer to the way a person demands in a wide variety of respects to keep information about herself protected from access, to control how it is passed on to others. If protecting what is private is then in general about controlling "access" to ones own person in various regards, this issue, as far as the question of informational privacy is concerned, must be understood and interpreted as control over what others can know about a person: this is consequently roughly what I would like to explain as "informational privacy."

At heart, it is about who knows what about another person and how they know it, i.e. about control over information affecting that person, and in this case control at least in the sense that a person in many respects has an idea of, or at least can guess what someone else knows about her: that she therefore can make well-founded assumptions about what persons or institutions she has contact with know about her and that, based on these assumptions and expectations,

she then has at her disposal the corresponding options to sanction or at least to criticize how she is handled.

One problem of informational privacy is thus the question of why we hold it to be a general right—variously specified according to context—or at least believe we have a well-founded claim not to be observed or listened to against our will and/or without our knowledge, or to control the extent of information that others have about us.

But why is the reference to the concepts of freedom and autonomy relevant here? One might object that when we observe or eavesdrop on people or talk about them, we evidently do not hinder their freedom in any way, at least their freedom is not *prima facie* restricted through these actions.

Why should I no longer do what I want to do just because others watch me or listen to me doing it, and why should the passing on of my "data" to others, as long as it is not tied to any actual restrictions, endanger my freedom, especially when I am not even aware of it and may never find out about it at all?

In order to now elucidate the crucial step that connects privacy, information control and autonomy, I would like to briefly describe to you a few examples.

[...]

The first example is designed to show how informational privacy can be violated in the public sphere by unwanted observation; it has to do with concealed video surveillance in public places. If you walk out onto the street to go shopping, you naturally do so in the expectation of showing yourself to other people, or coming into contact with others. You expect, you take for granted, that others will see, register how you look today, what you're wearing; you expect to perhaps run into people you know, or to chat at the cash register with perfect strangers. But you do not expect these events to be recorded on film and thus rendered reproducible, presentable outside their context in place or time, analyzable, communicable, controllable.

If you knew you were being watched, you might behave differently or at least act in the consciousness of being filmed. And it is this difference that shows that we can and should speak in cases of violation of informational privacy of an infringement on autonomy. Even if someone never finds out that she has been observed or filmed, her behavior was nonetheless then behavior "under false pretenses"; it is not really self-determined behavior because the assumptions she was making were false.

Another example has to do with the transmission of data, for example of medical data. If, for example, my employer enlists the help of experts (my doctor or health insurance fund) to find out information on my medical history, he not only violates my expectation that my medical data is privy only to my doctor and perhaps my insurance company, apart from persons I personally inform; he also of course limits my possibilities for self-determined behavior, for control of how I present myself, for authentic behavior in the occupational context. My employer now knows something about me, has information about me I don't know he has, but which is vital to the way I present myself to him, to my communication with him, and thus also to my self-determined behavior toward him. This is at any rate the case when I find out about the deception, but even if I only suspect that I have been thus betrayed, or if I can no longer be sure that my information has not been shared, my possibilities for self-determined behavior might nonetheless be massively restricted.

These examples now point up in my view a more wide-ranging and *general* thesis: The protection of informational privacy is so important for people because it is a constituent part of their self-understanding as autonomous persons. It allows them (within bounds) to exercise control

over their own self-portrayal, i.e. to control how they present themselves to whom in which contexts, how they "stage" or show themselves, which role they take in particular contexts and how they want to be perceived in that role, and therefore also how they want to act in a given context.

[...]

The presence of or observation by others can hence compel us to take notice of this fact, i.e. that others are there or that we are being watched. And respecting people's privacy then means conversely accepting that one's own behavior and knowledge might under certain circumstances influence the actions of others in an undesirable way.

Respect for a person's privacy is thus respect for her as an autonomous subject—that is the vital insight here. Therefore, in order to behave in a self-determined fashion, we must in general believe and be able to presume that we are not being observed, eavesdropped on, deceived about what data is collected and shared with others, or about the presence of others, and about what those present know about us and "who" they are therefore "for us." For the same reason, it is no use if people know they are being watched or that information on them is being stored if they do not want to be observed or registered in this manner—because it is then precisely the fact that they have to adapt to this observation and control that prevents them from acting in a self-determined, authentic way. If we analyze the field of informational privacy in this way, then it is clear that we are not talking here only of issues such as the state conducting bugging operations against its citizens, but in principle about all interpersonal relationships.

We have thus, I think, adequately illuminated the connection between autonomy and informational privacy and have revealed and established a normative basis for the protection of informational privacy. Now let me address the next question: Under what circumstances do these sorts of normative considerations actually become relevant?

The public or private structure of control over knowledge that other people have, as described above, or over knowledge that they show or do not show—this whole structure has of course always been regulated conventionally through the social, legal and conventional lines separating what is private from what is public. The justification for my expectations of how my interaction partner behaves and what he knows lies in the validity of social and legal conventions and norms that regulate—sometimes in very different ways from culture to culture—what is regarded in each case as worthy of protection and intimate, what is deemed as the legitimate realm or protective shield guarding the person from public view or control, and hence what should be subject to individual information control and what should not. These expectations are regulated through a complicated, but relatively stable fabric of social and legal norms and conventions within which we can act and master the various relationships in which we live. The question as to the basis for these norms and conventions only becomes relevant when they themselves are called into question, criticized, become dysfunctional, limiting or simply no longer fitting, or are described or perceived as no longer adequate.

And it is just this situation of *upheaval of norms and conventions* in which the current problem of informational privacy must be localized. [...] We have this kind of situation of upheaval, or to put it more mildly, of change and the questioning of prior norms and conventions, when, for example, new situations (e.g. terrorist acts) prompt the state to resort to measures that conflict with the protection of citizens' informational privacy. We also have the same kind of situation when methods are discovered and new areas developed in which technological advances exceed the bounds of our traditional concepts and applications of private and public, as is the case in the so-called panoptic society. And finally, we have this situation when new formats and taboo

violations are developed in the media that play with the de-privatization of themes and modes of behavior that were formerly kept private and considered intimate.
And that brings us to our first example, the new security laws. I just want to briefly touch on and discuss one element here, the problem of incorporating biometric data into passports. What we can see based on this small example is that a potential infringement of informational privacy can have much wider implications than merely the violation itself.
One might of course simply claim that it is irrelevant if your passport lists the shape of your iris alongside the color of your eyes. It might in principle not matter to you which personal data the state collects on you, as long as the data is not misused.
But you would then be missing the point of what is at risk with informational privacy. The problem is namely not only the risk of a possible violation of informational privacy, although this is also critical. The collection of personal data not only opens the door to possible misuse; the greater the mass of data stored on us, the more vulnerable we are. What is also problematic here is that the liberal state is presenting itself here as one that is able to and wants to have unlimited access to its citizens. So one must also consider the problem of biometric data registration and with it the problem of informational privacy from the perspective of how far the state can fulfill its role as guarantor of autonomy, of the negative as well as positive freedom of its citizens.
Namely, there is also the danger that, due to a structural state-initiated or societal disdain for the protection of informational privacy, people might for this very reason tend not to regard their own autonomy as relevant. The democratic constitutional state in particular, which the respective interior ministers are at pains to safeguard with their measures, can live only on the basis of citizens who place a very high value on their own individual autonomy. Liberal democracies must, for strategic reasons alone, have a massive interest in their legal subjects being extremely invested in self-determination, since their functioning would otherwise be jeopardized. If private autonomy is violated, this ultimately also affects the public autonomy of the democracy itself. Of course there are conflicts such as the one between the state's necessary duty to protect its citizens from terrorism and its task to protect the individual liberty of these very same citizens—the reality of such conflicts cannot be disputed. But they should at least be described correctly. If the right to freedom and the interest in autonomy are defended on the one side, there must not only be a very compelling reason (such as fighting terrorists) to violate them, but the measures taken must also demonstrate a high degree of effectiveness in achieving the desired goal to make them appear worthwhile. This is precisely what does not seem to be the case for the new security regulations and registration of personal data.
Let us now look at the second example, the development of new information technologies in our so-called panoptic society. As is well known, the term and idea behind the panopticon originally comes from Bentham and made its way into today's debates on informational privacy via Foucault. Foucault's panopticon is only interesting here insofar as it provides a visualization of "invisible power" that "penetrates deeper and deeper into people's behavior," of the "automatic functioning of power," which we can use to elucidate the question of what is problematic about the rapid development of the latest information technologies and by extension about the risk to *informational privacy.* The problem is obviously that one can as a matter of course always be identified as a certain person and then, just as matter-of-factly and constantly, be monitored. And we are not talking here (despite Foucault) about being observed, controlled and identified by an Orwellian surveillance state, or at least not only about this, but also about the opportunities that in principle every individual has with regard to everyone else—the shop owner vis-à-

vis his customers, the parents vis-à-vis the babysitter, the insurance companies vis-à-vis their policyholders, hackers vis-à-vis all other Internet surfers. So it is not just about the power of the state here; this power can also take an egalitarian form, the power to violate informational privacy. This is an egalitarian power that makes it difficult to determine here who is excluded and who is excluding. And this is the kind of power that doesn't even have to be put to use in order to be effective. It does not have to be used *a fortiori* with the aim of harming others—curiosity alone, for example, is a comparatively harmless motive. The problem is above all the effect of these possibilities, about the fact that one *can* in principle be seen, traced, described and therewith controlled.

This is therefore how we should understand one side of the danger. But this danger has another side as well: in this extremely wide-ranging field of relevant data in the services sector, it is particularly complicated to speak unambiguously of conflicts and violations of informational privacy because people increasingly tend to voluntarily forfeit their privacy depending on the cost/benefit ratio involved. In some cases they even use their privacy as a negotiation tool or "sell" it. Not only do all those who surf the Internet or pay with a credit card, order items from webshops, etc. daily and voluntarily forfeit certain areas of their privacy—and here we need only think of the routine installation of cookies on PCs. What's more, these people can easily turn the tables and quickly learn techniques to intrude on the privacy of others in the Internet.

[...]

The dangers thus lie on the one hand in a voluntary renunciation of informational privacy, and on the other in the involuntary possibility of control. We can and should view both as problematic because both—the voluntary and the involuntary decline in the protection of informational privacy—can not only make it more difficult to realize certain forms and dimensions of self-determined and authentic behavior, but can also lead to such behavior being regarded as less relevant, less central, less constitutive for a successful life. If, and to the extent that, we forfeit the right to remain unobserved, unidentifiable and inaccessible in important aspects of our lives, this would mean that our self-image as persons has changed. This then affects not only the idea of a successful—self-determined—life, but also the idea of liberal democracy itself, which depends on autonomous subjects who are conscious of and value this autonomy.

Translated from German by Jennifer Taylor-Gaida

The following thoughts represent a reworked version of an article that appeared in the book *Privat! Kontrollierte Freiheit in einer vernetzten Welt* (edited by Ralf Grötker, Heise Zeitschriften Verlag 2003); similar themes are addressed in much more detail in my book *Der Wert des Privaten* (Frankfurt: Suhrkamp 2001; English translation published by Polity Press 2005, *The Value of Privacy)*.